

Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1. (Currently Amended) A method of identifying unwanted messages, the method comprising:
 - inspecting a payload portion of a message being communicated and identifying characteristics of the payload portion;
 - comparing the characteristics of the inspected payload portion of the message with stored data indicating characteristics of at least one other message that has been inspected; and
 - based on comparison results, identifying a security condition ~~based on the comparison~~ from among at least one of acceptable, unacceptable, and indeterminate states; and
 - processing the message based on the security condition, wherein processing the message includes:
 - rejecting the message if the security condition associated with the message reflects the unacceptable state;
 - accepting the message if the security condition associated with the message reflects the acceptable state; and
 - if the security condition associated with the message reflects the indeterminate state, monitoring the message by:
 - tracking a location of the message;
 - inspecting at least one other message subsequent to the processing of the message;
 - updating the stored data to indicate characteristics of the at least one other message that has been inspected;

recategorizing the security condition of the message based on the updated
stored data; and
reprocessing the message based on the security condition.

2. (Original) The method of claim 1 wherein the characteristics of the payload portion include information other than address information.

3. (Original) The method of claim 2 wherein the characteristics of the payload portion do not include address information.

4. (Original) The method of claim 1 wherein the message includes an electronic mail message.

5. (Cancelled) The method of claim 1 further comprising rejecting the message if the security condition identified includes a hostile indicator.

6. (Currently Amended) The method of claim 5 wherein the security condition associated with a message is identified as reflecting a hostile indicator the unacceptable state when the comparison of the characteristics reveals a threshold number of messages having a shared characteristic.

7. (Currently Amended) The method of claim 6 ~~further comprising wherein~~ reprocessing the message based on the security condition includes removing previously accepted messages having characteristics in common with subsequently exchanged messages the message if the security condition associated with the at least one other message inspected subsequent to the processing of the message for which the security condition is identified as including reflecting the hostile indicator the unacceptable state and the at least one other message has characteristics in common with the message.

8. (Original) The method of claim 1 further comprising tracking the characteristics of the payload portion for comparison against characteristics of future messages, wherein the characteristics of a new message are compared with the characteristics of at least one message that has been tracked.

9. (Currently Amended) The method of claim ~~8~~7 wherein comparing the characteristics of the payload portion includes comparing the characteristics of the payload portion of messages inspected with stored characteristics of other communicated messages.

10. (Currently Amended) The method of claim ~~8~~7 wherein the characteristics of the payload portion of a message is ~~are~~ tracked when the security condition is identified as including reflecting ~~the~~an indeterminate state indicator.

11. (Currently Amended) The method of claim 10 wherein ~~the~~ an indeterminate state indicator is identified if the comparison of the characteristics does not itself reveal an unacceptable a hostile security condition, but the characteristics of the payload portion would reveal ~~a hostile security condition~~ the unacceptable state in combination with similar characteristics of other messages.

12. (Currently Amended) The method of claim 10 further comprising accepting the message if the security condition associated with the message reflects the indeterminate state ~~includes the indeterminate indicator~~.

13. (Cancelled) The method of claim 1 further comprising accepting the message if the security condition includes a neutral indicator.

14. (Original) The method of claim 1 wherein identifying the security condition includes comparing the characteristics of more than one message received by a single device.

15. (Original) The method of claim 1 wherein identifying the security condition includes comparing the characteristics of more than one message sent by a single device.

16-29. (Cancelled).

30. (New) The method of claim 1 wherein recategorizing the security condition of the message includes identifying the security condition as reflecting the acceptable state.

31. (New) The method of claim 1 wherein recategorizing the security condition of the message includes identifying the security condition as reflecting the unacceptable state.

32. (New) The method of claim 1 wherein identifying the security condition as reflecting the acceptable state includes identifying the security condition as reflecting a neutral state.

33. (New) The method of claim 1 wherein identifying the security condition as reflecting the unacceptable state includes identifying the security condition as reflecting a hostile state.

34. (New) The method of claim 1 wherein recategorizing the security condition of the message is performed when the stored data is updated such that the security condition associated with a message with certain characteristics would be identified as reflecting a state other than the indeterminate state and the security condition associated with the message with the same characteristics would have been identified as reflecting the indeterminate state prior to the update.

35. (New) The method of claim 1 wherein recategorizing the security condition of the message is performed if at least one other message inspected subsequent to the processing of the message includes a characteristic that increases the number of messages inspected with that characteristic above a threshold level.

36. (New) The method of claim 1 wherein recategorizing the security condition of the message is performed when the stored data is updated such that an alarm score of at one least one characteristic of a message increases.

37. (New) The method of claim 1 wherein recategorizing the security condition of the message is performed when the stored data is updated such that an alarm score of at one least one characteristic of a message decreases.

38. (New) The method of claim 1 wherein recategorizing the security condition of the message is performed when an administrator updates the stored data to indicate that at least one characteristic of a message is acceptable.

39. (New) The method of claim 1 wherein recategorizing the security condition of the message is performed when an administrator updates the stored data to indicate that at least one characteristic of a message is unacceptable.

40. (New) The method of claim 1 wherein reprocessing the message includes removing the message from storage if the security condition includes the unacceptable state.

41. (New) The method of claim 1 wherein reprocessing the message includes generating an alarm if the security condition reflects the unacceptable state.

42. (New) The method of claim 1 wherein reprocessing the message includes continuing to track the location of the message if the security condition still reflects the indeterminate state.

43. (New) The method of claim 1 wherein recategorizing the message includes:
accessing the location of the message;
retrieving the message from the location;
inspecting a payload portion of the message and identifying characteristics of the payload portion;
comparing the characteristics of the payload portion of the message with the updated stored data; and
in response to comparing, identifying the security condition from among at least one of the acceptable, unacceptable, and indeterminate states.

44. (New) A method of determining a definitive classification of a first message, the method comprising:
comparing at least one characteristic of the first message being communicated with a set of rules used in determining classification of messages;
in response to comparing, determining whether the first message is associated with a definitive classification;
tracking the first message as a tracked message if the first message is not associated with a definitive classification; and
subsequently attempting to determine the definitive classification for the tracked message if the set of rules has been updated.

45. (New) The method of claim 44 further comprising:

continuing to track the first message as a tracked message if determining whether the first message is associated with the definitive classification for the tracked message fails to indicate a definitive classification for the tracked message.

46. (New) The method of claim 44 further comprising:
processing the first message based on the classification of the first message if the first message is determined to be associated with the definitive classification.

47. (New) The method of claim 44 wherein the first message is determined to be associated with the definitive classification if a security condition associated with the first message is associated with an acceptable state.

48. (New) The method of claim 44 wherein the first message is determined to be associated with the definitive classification if a security condition associated with the first message is associated with an unacceptable state.

49. (New) The method of claim 44 wherein the first message is determined to be associated with the definitive classification if a security condition associated with the first message is associated with a neutral state.

50. (New) The method of claim 44 wherein the first message is determined to be associated with the definitive classification if a security condition associated with the message is associated with a hostile state.

51. (New) The method of claim 44 wherein the first message is not determined to be associated with the definitive classification if a security condition associated with the first message is associated with an indeterminate state.